Claims

What is claimed is:

1. A method for generating a random number, comprising the steps of:

operating a plurality of flip-flops in a meta-stable state;

generating a random bit if one of said flip-flops enter said meta-stable state; and

preventing the generation of a random bit if more than one of said plurality of flip-flops enter a meta-stable state within a predefined time interval.

2. The method of claim 1, wherein said flip-flops are driven in parallel.

3. The method of claim 1, wherein at lease one of said flip-flops is connected to at least one other of said flip-flops.

4. The method of claim 1, wherein said preventing step is performed by one or more exclusive or (XOR) circuits.

5. The method of claim 1, wherein said generating step further comprises the step of choosing a random bit if an output of one of said flip-flops does not match an applied input.

6. The method of claim 1, further comprising the step of synchronizing an output of each of said flip-flops with a local clock source.

7. The method of claim 6, wherein a synchronizing circuit that performs said synchronizing step is less susceptible to becoming meta-stable than said flip-flips.

8. The method of claim 1, further comprising the step of collecting a plurality of said random bits to produce a random number.

9. The method of claim 1, further comprising the step of inverting an input signal for a second flip-flop to ensure that said second flip-flop does not have the same input signal as a first flip-flop.

10. A random number generator, comprising:

a plurality of flip-flops operated in a meta-stable state to generate a random bit if one of said flip-flops enter said meta-stable state; and

means for preventing the generation of a random bit if more than one of said plurality of flip-flops enter a meta-stable state within a predefined time interval.

11. The random number generator of claim 10, wherein said flip-flops are driven in parallel.

12. The random number generator of claim 10, wherein at least one of said flip-flops is connected to at least one other of said flip-flops.

13. The random number generator of claim 10, wherein said means for preventing the generation of a random bit is one or more exclusive or (XOR) circuits.

14. The random number generator of claim 10, wherein detection of the meta-stable state of said flip-flops is discerned if an output of one of said flip-flops does not match an applied input.

15. The random number generator of claim 10, further comprising a synchronizing circuit to synchronize an output of each of said flip-flops with a local clock source.

16. The random number generator of claim 15, wherein said synchronizing circuit is less susceptible to becoming meta-stable than said flip-flips.

17. The random number generator of claim 10, wherein a plurality of said random bits are collected to produce a random number.

18. A method for generating a random number, comprising the steps of:

operating a first flip-flop in a meta-stable state; and

generating a random bit from an output of a second flip flop when said first flip-flop is in said meta-stable state.

19. The method of claim 18, wherein said generating step is triggered by at least one exclusive or (XOR) circuit.

20. The method of claim 18, further comprising the step of synchronizing an output of said second flip-flop with a local clock source.

21. The method of claim 18, further comprising the step of collecting a plurality of said random bits to produce a random number.